

BEST AVAILABLE COPY

09/28/2001 09:20 FAX 415 384 0134

KEKER & VAN NEST LLP

002

1 WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
2 MARK R. WEINSTEIN (State Bar No. 193043)
ORRICK, HERRINGTON & SUTCLIFFE LLP

3 1000 Marsh Road
Menlo Park, CA 94025
4 Telephone: (650) 614-7400
Facsimile: (650) 614-7401

5 STEVEN ALEXANDER (admitted *Pro Hac Vice*)
6 KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
7 JOHN D. VANDENBERG (admitted *Pro Hac Vice*)
KLARQUIST SPARKMAN, LLP

8 One World Trade Center, Suite 1600
121 S.W. Salmon Street
9 Portland, OR 97204
Telephone: (503) 226-7391
10 Facsimile: (503) 228-9446

11 Attorneys for Defendant
MICROSOFT CORPORATION

12
13 UNITED STATES DISTRICT COURT
14 NORTHERN DISTRICT OF CALIFORNIA
15 OAKLAND DIVISION
16

17 INTERTRUST TECHNOLOGIES
CORPORATION, a Delaware corporation,

18 Plaintiff,

19 v.

20 MICROSOFT CORPORATION, a
21 Washington Corporation,

22 Defendant.

CASE NO: C 01-1640 SBA

**MICROSOFT CORPORATION'S
FIRST AMENDED ANSWER AND
COUNTERCLAIMS TO THE SECOND
AMENDED COMPLAINT**

23
24 Defendant Microsoft Corporation ("Microsoft") answers the Second Amended
25 Complaint of InterTrust Technologies Corporation ("InterTrust") as follows:

26 1. Microsoft admits that the Second Amended Complaint purports to state a
27 cause of action under the patent laws of the United States, 35 United States Code, §§ 271 and

28 281. Microsoft denies that it has infringed or now infringes the patents asserted against Microsoft

DOCSSV1:160096.1

ORRICK
HERRINGTON
& SUTCLIFFE LLP

MICROSOFT CORPORATION'S FIRST AMENDED ANSWER
AND COUNTERCLAIMS. CASE NO. C 01-1640 SBA

1 in the Second Amended Complaint. Microsoft denies any and all remaining allegations of
2 paragraph 1 of the Second Amended Complaint.

3 2. Microsoft admits that the Second Amended Complaint purports to state a
4 cause of action over which this Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and
5 1338(a).

6 3. Microsoft admits, for purposes of this action only, that venue is proper in
7 this judicial district. Microsoft denies any and all remaining allegations of paragraph 3 of the
8 Second Amended Complaint.

9 4. Upon information and belief, Microsoft admits the allegations of paragraph
10 4 of the Second Amended Complaint.

11 5. Microsoft admits the allegations of paragraph 5 of the Second Amended
12 Complaint.

13 6. Microsoft admits, for purposes of this action only, that it transacts business
14 in this judicial district. Microsoft denies any and all remaining allegations of paragraph 6 of the
15 Second Amended Complaint.

16 7. Microsoft admits that on its face the title page of U.S. Patent No. 6,185,683
17 B1 ("the '683 Patent") states that it was issued February 6, 2001, is entitled "Trusted and secure
18 techniques, systems and methods for item delivery and execution," and lists "InterTrust
19 Technologies Corp." as the assignee. Microsoft admits that a copy of the '683 Patent was
20 attached to the copy of the Second Amended Complaint delivered to counsel for Microsoft, but
21 denies that such copy was full and complete insofar as it did not include any material purportedly
22 incorporated by reference therein. Microsoft denies that the '683 Patent was duly and lawfully
23 issued. Microsoft further denies any and all remaining allegations of paragraph 7 of the Second
24 Amended Complaint.

25 8. Microsoft admits that on its face the title page of U.S. Patent No. 6,253,193
26 B1 ("the '193 Patent") states that it was issued June 26, 2001, is entitled "Systems and methods
27 for the secure transaction management and electronic rights protection," and lists "InterTrust
28 Technologies Corporation" as the assignee. Microsoft admits that a copy of text associated with
DOCS5V1:160096.1

BEST AVAILABLE COPY

09/28/2001 09:21 FAX 415 394 0134

KEKER & VAN NEST LLP

004

1 the '193 Patent was attached to the copy of the Second Amended Complaint delivered to counsel
2 for Microsoft, but denies that such copy was full and complete as it did not include, among other
3 things, any of the drawings or figures. Microsoft further denies such copy was full and complete
4 insofar as it did not include any material purportedly incorporated by reference therein. Microsoft
5 denies that the '193 Patent was duly and lawfully issued. Microsoft further denies any and all
6 remaining allegations of paragraph 8 of the Second Amended Complaint.

7 9. Microsoft admits that on its face the title page of U.S. Patent No. 5,940,504
8 ("the '504 Patent") states that it was issued August 17, 1999 and is entitled "Licensing
9 management system and method in which datagrams including an addressee of a licensee and
10 indicative of use of a licensed product are sent from the licensee's site." Microsoft admits that a
11 copy of the '504 Patent was attached to the copy of the Second Amended Complaint delivered to
12 counsel for Microsoft. Microsoft denies that the '504 Patent was duly and lawfully issued.
13 Microsoft further denies any and all remaining allegations of paragraph 9 of the Second Amended
14 Complaint.

15 10. Microsoft admits that on its face the title page of U.S. Patent No. 5,920,861
16 ("the '861 Patent") states that it was issued July 6, 1999, is entitled "Techniques for defining,
17 using and manipulating rights management data structures," and lists "InterTrust Technologies
18 Corp." as the assignee. Microsoft admits that a copy of the '861 Patent was attached to the copy
19 of the Second Amended Complaint delivered to counsel for Microsoft, but denies that such copy
20 was full and complete insofar as it did not include any material purportedly incorporated by
21 reference therein. Microsoft denies that the '861 Patent was duly and lawfully issued. Microsoft
22 further denies any and all remaining allegations of paragraph 10 of the Second Amended
23 Complaint.

24 11. Microsoft repeats and reasserts its responses to paragraphs 1-7 of the
25 Second Amended Complaint, as if fully restated herein.

26 12. Microsoft admits that the Second Amended Complaint purports to state a
27 cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now
28 infringes the patents asserted against Microsoft in the Second Amended Complaint. Microsoft

DOCSSV1:16C096.1

ORRICK
HERRINGTON
& SUTCLIFFE LLP
SILICON VALLEY

BEST AVAILABLE COPY

09/28/2001 09:21 FAX 415 394 0134

KEKER & VAN NEST LLP

005

1 denies any and all remaining allegations of paragraph 12 of the Second Amended Complaint.
2 13. Microsoft denies any and all allegations of paragraph 13 of the Second
3 Amended Complaint.
4 14. Microsoft denies any and all allegations of paragraph 14 of the Second
5 Amended Complaint.
6 15. Microsoft denies any and all allegations of paragraph 15 of the Second
7 Amended Complaint.
8 16. Microsoft denies any and all allegations of paragraph 16 of the Second
9 Amended Complaint.
10 17. Microsoft denies any and all allegations of paragraph 17 of the Second
11 Amended Complaint.
12 18. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 8 of the
13 Second Amended Complaint, as if fully restated herein.
14 19. Microsoft admits that the Second Amended Complaint purports to state a
15 cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now
16 infringes the patents asserted against Microsoft in the Second Amended Complaint. Microsoft
17 denies any and all remaining allegations of paragraph 19 of the Second Amended Complaint.
18 20. Microsoft denies any and all allegations of paragraph 20 of the Second
19 Amended Complaint.
20 21. Microsoft denies any and all allegations of paragraph 21 of the Second
21 Amended Complaint.
22 22. Microsoft denies any and all allegations of paragraph 22 of the Second
23 Amended Complaint.
24 23. Microsoft denies any and all allegations of paragraph 23 of the Second
25 Amended Complaint.
26 24. Microsoft denies any and all allegations of paragraph 24 of the Second
27 Amended Complaint.

28
ORRICK
HERRINGTON
& SUTCLIFFE LLP

DOCSSV1:160096.1

-4-

MICROSOFT CORPORATION'S FIRST AMENDED ANSWER
AND COUNTERCLAIMS, CASE NO. C 01-1640 SBA

BEST AVAILABLE COPY

09/28/2001 09:21 FAX 415 394 0134

KEKER & VAN NEST LLP

006

1 25. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 9 of the
2 Second Amended Complaint, as if fully restated herein.

3 26. Microsoft admits that the Second Amended Complaint purports to state a
4 cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now
5 infringes the patents asserted against Microsoft in the Second Amended Complaint. Microsoft
6 denies any and all remaining allegations of paragraph 26 of the Second Amended Complaint.

7 27. Microsoft denies any and all allegations of paragraph 27 of the Second
8 Amended Complaint.

9 28. Microsoft denies any and all allegations of paragraph 28 of the Second
10 Amended Complaint.

11 29. Microsoft denies any and all allegations of paragraph 29 of the Second
12 Amended Complaint.

13 30. Microsoft denies any and all allegations of paragraph 30 of the Second
14 Amended Complaint.

15 31. Microsoft denies any and all allegations of paragraph 31 of the Second
16 Amended Complaint.

17 32. Microsoft repeats and reasserts its responses to paragraphs 1-6 and 10 of
18 the Second Amended Complaint, as if fully restated herein.

19 33. Microsoft admits that the Second Amended Complaint purports to state a
20 cause of action under 35 U.S.C. §§ 271 and 281. Microsoft denies that it has infringed or now
21 infringes the patents asserted against Microsoft in the Second Amended Complaint. Microsoft
22 denies any and all remaining allegations of paragraph 33 of the Second Amended Complaint.

23 34. Microsoft denies any and all allegations of paragraph 34 of the Second
24 Amended Complaint.

25 35. Microsoft denies any and all allegations of paragraph 35 of the Second
26 Amended Complaint.

27 36. Microsoft denies any and all allegations of paragraph 36 of the Second
28 Amended Complaint.

DOC5V1:160096.1

BEST AVAILABLE COPY

09/28/2001 09:22 FAX 415 394 0134

KEKER & VAN NEST LLP

007

1 37. Microsoft denies any and all allegations of paragraph 37 of the Second
2 Amended Complaint.

3 38. Microsoft denies any and all allegations of paragraph 38 of the Second
4 Amended Complaint.

AFFIRMATIVE AND OTHER DEFENSES

5
6 Further answering the Second Amended Complaint, Microsoft asserts the
7 following defenses. Microsoft reserves the right to amend its answer with additional defenses as
8 further information is obtained.

First Defense: Noninfringement of the Asserted Patents

9
10 1. Microsoft has not infringed, contributed to the infringement of, or induced
11 the infringement of U.S. Patent No. 6,185,683 B1 ("the '683 Patent"), U.S. Patent No. 6,253,193
12 B1 ("the '193 Patent"), U.S. Patent No. 5,940,504 ("the '504 Patent") or U.S. Patent No.
13 5,920,861 ("the '861 Patent"), and is not liable for infringement thereof.

14 2. Any and all Microsoft products or actions that are accused of infringement
15 have substantial uses that do not infringe and therefore cannot induce or contribute to the
16 infringement of the '683 Patent, the '193 Patent, the '504 Patent or the '861 Patent.

Second Defense: Invalidity of the Asserted Patents

17
18 3. On information and belief, the '683 Patent, the '193 Patent, the '504 Patent
19 and the '861 Patent are invalid for failing to comply with the provisions of the Patent Laws, Title
20 35 U.S.C., including without limitation one or more of 35 U.S.C. §§ 102, 103 and 112.

Third Defense: Unavailability of Relief

21
22 4. On information and belief, Plaintiff has failed to plead and meet the
23 requirements of 35 U.S.C. § 271(b) and is not entitled to any alleged damages prior to providing
24 any actual notice to Microsoft of the '683 Patent, the '193 Patent, the '504 Patent or the '861
25 Patent.

Fourth Defense: Unavailability of Relief

26
27 5. On information and belief, Plaintiff has failed to plead and meet the
28 requirements of 35 U.S.C. § 284 for enhanced damages and is not entitled to any damages prior to

DOCSSV1:160096.1

ORRICK
HERRINGTON
& SUTCLIFF LLP

-6-

MICROSOFT CORPORATION'S FIRST AMENDED ANSWER
AND COUNTERCLAIMS. CASE NO. C 01-1640 SBA

1 providing any actual notice to Microsoft of the '683 Patent, the '193 Patent, the '504 Patent,
2 and/or the '861 Patent, and any alleged infringement thereof.

3 **Fifth Defense: Unavailability of Relief**

4 6. On information and belief, Plaintiff has failed to plead and meet the
5 requirements of 35 U.S.C. § 287, and has otherwise failed to show that it is entitled to any
6 damages.

7 **Sixth Defense: Prosecution History Estoppel**

8 7. Plaintiff's alleged causes of action for patent infringement are barred under
9 the doctrine of prosecution history estoppel, and Plaintiff is estopped from claiming that the '683
10 Patent, the '193 Patent, the '504 Patent, and/or the '861 Patent covers or includes any accused
11 Microsoft product or method.

12 **Seventh Defense: Dedication to the Public**

13 8. Plaintiff has dedicated to the public all methods, apparatus, and products
14 disclosed in the '683 Patent, the '193 Patent, the '504 Patent, and/or the '861 Patent, but not
15 literally claimed therein, and is estopped from claiming infringement by any such public domain
16 methods, apparatus, and products.

17 **Eighth Defense: Use/Manufacture By/For United States Government**

18 9. To the extent that any accused product has been used or manufactured by
19 or for the United States, Plaintiff's claims and demands for relief are barred by 28 U.S.C. § 1498.

20 **Ninth Defense: License**

21 10. To the extent that any of Plaintiff's allegations of infringement are
22 premised on the alleged use, sale, or offer for sale of products that were manufactured by or for a
23 licensee of InterTrust and/or provided by or to Microsoft to or by a licensee of InterTrust, such
24 allegations are barred pursuant to license.

25 **Tenth Defense: Acquiescence**

26 11. Plaintiff has acquiesced in at least those acts of Microsoft that are alleged
27 to infringe the '861 Patent, the '683 Patent, and the '193 Patent.

Eleventh Defense: Laches

12. Plaintiff's claims for relief are barred, in whole or in part, by the equitable doctrine of laches.

Twelfth Defense: Inequitable Conduct

13. The '861 Patent claims are unenforceable due to inequitable conduct, including those acts and failures to act set forth in Microsoft's Counterclaim for Declaratory Judgment of Unenforceability of the '861 Patent, set forth below.

COUNTERCLAIMS

COUNT I - DECLARATORY
JUDGMENT OF NONINFRINGEMENT

1. This action arises under the patent laws of the United States, Title 35 U.S.C. §§ 1, et seq. This Court has subject matter jurisdiction over this counterclaim under 28 U.S.C. §§ 1338, 2201, and 2202.

2. Microsoft Corporation ("Microsoft") is a Washington corporation with its principal place of business in Redmond, Washington.

3. Upon information and belief, Plaintiff/Counterclaim Defendant InterTrust Technologies Corporation ("InterTrust") is a Delaware corporation with its principal place of business in Santa Clara, California.

4. InterTrust purports to be the owner of U.S. Patent Nos. 6,185,683 B1 ("the '683 Patent"), 6,253,193 B1 ("the '193 Patent"), 5,940,504 ("the '504 Patent"), and 5,920,861 ("the '861 Patent").

5. InterTrust alleges that Microsoft has infringed the '683 Patent, the '193 Patent, the '504 Patent, and the '861 Patent.

6. No Microsoft product has infringed, either directly or indirectly, any claim of the '683 Patent, the '193 Patent, the '504 Patent, or the '861 Patent, and Microsoft is not liable for infringement thereof.

///

BEST AVAILABLE COPY

09/28/2001 09:22 FAX 415 394 0134

KEKER & VAN NEST LLP

010

1 7. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202,
2 exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to the
3 infringement or noninfringement of the '683 Patent, the '193 Patent, the '504 Patent, and/or the
4 '861 Patent.

5 COUNT II - DECLARATORY 6 JUDGMENT OF INVALIDITY OF THE '683 PATENT

7 8. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if
8 fully restated herein.

9 9. The '683 Patent, and each claim thereof, is invalid for failing to comply
10 with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

11 10. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202,
12 exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to
13 whether the claims of the '683 Patent are valid or invalid.

14 COUNT III - DECLARATORY 15 JUDGMENT OF INVALIDITY OF THE '193 PATENT

16 11. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if
17 fully restated herein.

18 12. The '193 Patent, and each claim thereof, is invalid for failing to comply
19 with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

20 13. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202,
21 exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to
22 whether the claims of the '193 Patent are valid or invalid.

23 COUNT IV - DECLARATORY 24 JUDGMENT OF INVALIDITY OF THE '504 PATENT

25 14. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if
26 fully restated herein.

27 15. The '504 Patent, and each claim thereof, is invalid for failing to comply
28 with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

1 16. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202,
2 exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to
3 whether the claims of the '504 Patent are valid or invalid.

**COUNT V - DECLARATORY
JUDGMENT OF INVALIDITY OF THE '861 PATENT**

4
5
6 17. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims as if
7 fully restated herein.

8 18: The '861 Patent, and each claim thereof, is invalid for failing to comply
9 with the provisions of the Patent Laws, including one or more of 35 U.S.C. §§ 102, 103 and 112.

10 19. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202,
11 exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to
12 whether the claims of the '861 Patent are valid or invalid.

**COUNT VI - DECLARATORY JUDGMENT
OF UNENFORCEABILITY OF THE '861 PATENT**

13
14
15 20. Microsoft repeats and realleges paragraphs 1-5 of its Counterclaims, as if
16 fully restated herein.

17 21. Claims 1-129 of the '861 Patent application (SN 08/805,804), and claims
18 1-101 of the '861 Patent, were not and are not entitled to benefit of any application filing date
19 prior to February 25, 1997, under 35 U.S.C. § 120 or otherwise.

20 22. Exhibit A hereto is a reprint of an article entitled "Digibox: A Self-
21 Protecting Container for Information Commerce." The article shown in Exhibit A (hereafter,
22 "the Sibert article") was published in July 1995 in the Proceedings of the First USENIX
23 Workshop on Electronic Commerce.

24 23. On information and belief, the content of pages 2-14 of Exhibit A was
25 presented at a public conference in the United States in July 1995.

26 24. Exhibit B hereto is a copy of a page from an International Application
27 published under the Patent Cooperation Treaty (PCT), bearing International Publication Number
28 WO 96/27155.

BEST AVAILABLE COPY

09/28/2001 09:23 FAX 415 394 0134

KEKER & VAN NEST LLP

012

1 25. On information and belief, International Application WO 96/27155 has, at
2 all times since its filing date, been owned and controlled by InterTrust or its predecessors in
3 interest.

4 26. International Application WO 96/27155 (hereafter "the WO 96/27155
5 (PCT) publication") was published on September 6, 1996.

6 27. United States Patent No. 5,910,987 ("the '987 Patent") issued on June 8,
7 1999, from a continuation of an application filed on February 13, 1995.

8 28. The Sibert article is prior art to claims 1-129 of the '861 Patent application
9 (SN 08/805,804), and claims 1-101 of the '861 Patent, under 35 U.S.C. §§ 102(b), 103.

10 29. The WO 96/27155 (PCT) publication is prior art to claims 1-129 of the
11 '861 Patent application (SN 08/805,804), and claims 1-101 of the '861 Patent, under 35 U.S.C. §§
12 102(a), 103.

13 30. The '987 Patent is prior art to claims 29-129 of the '861 Patent application
14 (SN 08/805,804), and claims 1-101 of the '861 Patent, under 35 U.S.C. §§ 102(e), 103.

15 31. The Sibert article was material to the patentability of claim 1 of the '861
16 Patent application (SN 08/805,804).

17 32. The Sibert article was material to the patentability of claims 2-129 of the
18 '861 Patent application (SN 08/805,804).

19 33. The WO 96/27155 (PCT) publication was material to the patentability of
20 claim 1 of the '861 Patent application (SN 08/805,804).

21 34. The WO 96/27155 (PCT) publication was material to the patentability of
22 claims 2-129 of the '861 Patent application (SN 08/805,804).

23 35. The '987 Patent was material to the patentability of claims 29-129 of the
24 '861 Patent application (SN 08/805,804).

25 36. One or more of the '861 Patent applicants knew, while the '861 Patent
26 application (SN 08/805,804) was pending, of the July 1995 publication of the Sibert article.

27 37. On information and belief, one or more of the '861 Patent applicants knew,
28 while the '861 Patent application (SN 08/805,804) was pending, of the September 1996

DOCSS\1:160096.1

ORRICK
HERRINGTON
& SUTCLIFF LLP

BEST AVAILABLE COPY

09/28/2001 09:23 FAX 415 394 0134

KEKER & VAN NEST LLP

013

1 publication of the WO 96/27155 (PCT) publication.

2 38. One or more of the '861 Patent applicants knew, while the '861 Patent
3 application (SN 08/805,804) was pending, of the June 8, 1999 issuance of the '987 patent.

4 39. On information and belief, one or more of the attorneys who prosecuted or
5 assisted in prosecuting the '861 Patent application (SN 08/805,804) knew, while that application
6 was pending, of the July 1995 publication of the Sibert article.

7 40. One or more of the attorneys who prosecuted or assisted in prosecuting the
8 '861 Patent application (SN 08/805,804) knew, while that application was pending, of the
9 September 1996 publication of the WO 96/27155 (PCT) publication.

10 41. One or more of the attorneys who prosecuted or assisted in prosecuting the
11 '861 Patent application (SN 08/805,804) knew, while that application was pending, of the June 8,
12 1999 issuance of the '987 patent.

13 42. The applicants for the '861 Patent did not cite the Sibert article, the WO
14 96/27155 (PCT) publication, or the '987 Patent to the Patent Office as prior art to any of claims 1-
15 129 of the '861 Patent application (SN 08/805,804).

16 43. The applicants for the '861 Patent did not cite to the Patent Office as prior
17 art to any of claims 1-129 of the '861 Patent application (SN 08/805,804) any reference having
18 the same or substantially the same disclosure as the Sibert article, the WO 96/27155 (PCT)
19 publication, or the '987 Patent.

20 44. None of the Sibert article, the WO 96/27155 (PCT) publication, or the '987
21 Patent is merely cumulative over any reference cited as prior art during the prosecution of the
22 '861 Patent application (SN 08/805,804).

23 45. On information and belief, one or more of the '861 Patent applicants
24 believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the
25 Sibert article disclosed an embodiment of claim 1 of the '861 Patent application (SN 08/805,804).

26 46. On information and belief, one or more of the '861 Patent applicants
27 believed, during pendency of claim 1 of the '861 Patent application (SN 08/805,804), that the
28 WO 96/27155 (PCT) publication disclosed an embodiment of claim 1 of the '861 Patent

DOCSSV1:160096.1

ORRICK
HERRINGTON
& SUTCLIFFE LLP

1 application (SN 08/805,804).

2 47. On information and belief, one or more of the '861 Patent applicants
3 believed, while the '861 Patent application (SN 08/805,804) was pending, that the Sibert article
4 was material to the patentability of claims 1-129 of the '861 Patent application (SN 08/805,804),
5 but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

6 48. On information and belief, one or more of the '861 Patent applicants
7 believed, while the '861 Patent application (SN 08/805,804) was pending, that the WO 96/27155
8 (PCT) publication was material to the patentability of claims 1-129 of the '861 Patent application
9 (SN 08/805,804), but, with deceptive intent, failed to disclose that reference as prior art to the
10 Patent Office.

11 49. On information and belief, one or more of the '861 Patent applicants
12 believed, while the '861 Patent application (SN 08/805,804) was pending, that the '987 Patent
13 was material to the patentability of claims 29-129 of the '861 Patent application (SN 08/805,804),
14 but, with deceptive intent, failed to disclose that reference as prior art to the Patent Office.

15 50. The '861 Patent is unenforceable due to the inequitable conduct of the '861
16 Patent applicants before the Patent and Trademark Office in connection with the '861 Patent
17 application (SN 08/805,804).

18 51. An actual controversy, within the meaning of 28 U.S.C. §§ 2201 and 2202,
19 exists between Microsoft, on the one hand, and InterTrust, on the other hand, with respect to
20 whether the claims of the '861 Patent are enforceable.

**COUNT VII - INFRINGEMENT
OF U.S. PATENT NO. 6,049,671**

23 52. Microsoft repeats and realleges paragraphs 2-3 of its Counterclaims, as if
24 fully restated herein.

25 53. This Court has exclusive subject matter jurisdiction over Microsoft's cause
26 of action for patent infringement under Title 28, United States Code, Sections 1331 and 1338, and
27 under the patent laws of the United States, Title 35 of the United States Code.

28

BEST AVAILABLE COPY

09/28/2001 09:24 FAX 415 394 0134

KEKER & VAN NEST LLP

015

1 54. U.S. Patent No. 6,049,671 ("the '671 Patent") issued to Microsoft
2 Corporation as the assignee of Benjamin W. Slivka and Jeffrey S. Webber on April 11, 2000.

3 55. A true copy of the '671 Patent is attached as Exhibit C hereto, and is
4 incorporated herein by reference.

5 56. Microsoft owns all right, title and interest in the '671 Patent.

6 57. InterTrust has had actual notice of the '671 Patent.

7 58. InterTrust has infringed one or more claims of the '671 Patent, in violation
8 of at least 35 U.S.C. § 271(a, b, c).

9 59. InterTrust's infringement of the '671 Patent has caused and will continue to
10 cause Microsoft damage, including irreparable harm for which it has no adequate remedy at law.

11 COUNT VIII - INFRINGEMENT 12 OF U.S. PATENT NO. 6,256,668

13 60. Microsoft repeats and realleges paragraphs 2-3 and 51 of its Counterclaims,
14 as if fully restated herein.

15 61. U.S. Patent No. 6,256,668 B1 ("the '668 Patent") issued to Microsoft
16 Corporation as the assignee of Benjamin W. Slivka and Jeffrey S. Webber on July 3, 2001.

17 62. A true copy of the '668 Patent is attached as Exhibit D hereto, and is
18 incorporated herein by reference.

19 63. Microsoft owns all right, title and interest in the '668 Patent.

20 64. InterTrust has had actual notice of the '668 Patent.

21 65. InterTrust has infringed one or more claims of the '668 Patent, in violation
22 of at least 35 U.S.C. § 271(a, b, c).

23 66. InterTrust's infringement of the '668 Patent has caused and will continue to
24 cause Microsoft damage, including irreparable harm for which it has no adequate remedy at law.

25 PRAYER FOR RELIEF

26 WHEREFORE, Microsoft prays for the following relief:

27 A. The Court enter judgment against InterTrust on, and dismiss with
28

BEST AVAILABLE COPY

09/28/2001 09:24 FAX 415 394 0134

KEKER & VAN NEST LLP

018

- 1 prejudice, any and all claims of the Second Amended Complaint;
- 2 B. The Court enter judgment declaring that Microsoft has not infringed,
- 3 contributed to infringement of, or induced infringement of the '683 Patent;
- 4 C. The Court enter judgment declaring that Microsoft has not infringed,
- 5 contributed to infringement of, or induced infringement of the '193 Patent;
- 6 D. The Court enter judgment declaring that Microsoft has not infringed,
- 7 contributed to infringement of, or induced infringement of the '504 Patent;
- 8 E. The Court enter judgment declaring that Microsoft has not infringed,
- 9 contributed to infringement of, or induced infringement of the '861 Patent;
- 10 F. The Court enter judgment declaring that the '683 Patent is invalid;
- 11 G. The Court enter judgment declaring that the '193 Patent is invalid;
- 12 H. The Court enter judgment declaring that the '504 Patent is invalid;
- 13 I. The Court enter judgment declaring that the '861 Patent is invalid;
- 14 J. The Court enter judgment that the '861 Patent is unenforceable due to
- 15 inequitable conduct;
- 16 K. The Court enter judgment that InterTrust has infringed the '671 patent;
- 17 L. The Court enter judgment that InterTrust has infringed the '668 patent;
- 18 M. A permanent injunction prohibiting InterTrust, its officers, agents, servants,
- 19 employees, and all persons in active concert or participation with them from infringing the '671
- 20 and '668 Patents;
- 21 N. An award against InterTrust of damages and attorney fees, pursuant to the
- 22 provisions of 35 U.S.C §§ 284, 285.
- 23 O. An award to Microsoft of prejudgment interest and the costs of this action.
- 24 P. The Court award to Microsoft its reasonable costs and attorneys' fees; and
- 25 Q. The Court grant to Microsoft such other and further relief as may be
- 26 deemed just and appropriate.

27 ///

28

ORRICK
HERRINGTON
& SUTCLIFFE LLP

DOCSSV1:160096.1

BEST AVAILABLE COPY

09/28/2001 09:25 FAX 415 394 0134

KEKER & VAN NEST LLP

017

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Defendant Microsoft Corporation demands a trial by jury.

DATED: September 17, 2001

By:

Mark R. Weinstein
WILLIAM L. ANTHONY
ERIC L. WESENBERG
MARK R. WEINSTEIN
ORRICK HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: 650-614-7400

STEVEN ALEXANDER
KRISTIN L. CLEVELAND
JAMES E. GERINGER
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391

Attorneys for Defendant
Microsoft Corporation

ORRICK
HERRINGTON
& SUTCLIFFE LLP

DOCSSV1:160096.1

BEST AVAILABLE COPY

09/28/2001 09:25 FAX 415 394 0134

KEKER & VAN NEST LLP

019



The following paper was originally published in the
Proceedings of the First USENIX Workshop on Electronic Commerce
New York, New York, July 1995.

DigiBox: A Self-Protecting Container for Information Commerce

Olin Sibert, David Bernstein, and David Van Wie
Electronic Publishing Resources, Inc.
Sunnyvale, California

For more information about USENIX Association contact:

1. Phone: 510 528-8649
2. FAX: 510 548-5738
3. Email: office@usenix.org
4. WWW URL: <http://www.usenix.org>

**The DigiBox:
A Self-Protecting Container for Information Commerce**

Olin Sibert
David Bernstein
David Van Wie

*Electronic Publishing Resources, Inc.
460 Oaknead Parkway
Sunnyvale, California
1 408 774 6100
info@epr.com*

Abstract

Information Commerce is a business activity carried out among several parties in which information carries value and is treated as a product. The information may be content, it may be returned usage and marketing data, and it may be representative of financial transactions.

In each of these cases the information is valuable and must be kept secure and private. Traditional approaches secure the transmission of that information from one point to another; there are no persistent protections. Protection of all of these components of information commerce for all parties in a transaction value chain is necessary for a robust electronic infrastructure.

A prerequisite to such an environment is a cryptographically protected container for packaging information and controls that enforce information rights. This paper describes such a container, called the DigiBox™. EPR has submitted initial specifications for the DigiBox container to the ANSI IISP Electronic Publishing Task Force (EPUB) within the User/Content Provider Standards Working Group (WG4).

1 Introduction

As services and products in modern commerce increasingly take electronic form, traditional commerce is evolving into electronic commerce. This includes both creation and enforcement of various agreements between parties in an electronic commercial relationship. It also includes enforcing the rights of these parties with respect to the secure management of electronic content or services usage, billing, payment, and related activities.

To save money, to be competitive, and to be efficient [1,2], members of modern society will shortly be using new information technology tools that

truly support electronic commerce. These tools provide for the flow of products and services through creators', providers', and users' hands. They enable the creation, negotiation, and enforcement of electronic agreements, including the evolution of controls that manage both the use and consequences of use of electronic content or services. In addition, these tools support "evolving" agreements that progressively reflect the requirements of further participants in a commercial model.

Participants in electronic commerce [3,4] will need rules and mechanisms such that:

1. Information providers can be assured that their content is used only in authorized ways;
2. Privacy rights of users of content are preserved; and
3. Diverse business models related to content can be electronically implemented.

The Internet and other information commerce infrastructures will require a management component that enforces such rules, ensuring a safe, coherent, fair, and productive community. This management component will be critical to the electronic highway's acceptance. Without rules to protect the rights of content providers and other electronic community members, the electronic highway will comprise nothing more than a collection of limited, disconnected applications.

Analysts have concluded that content will constitute the largest revenue-generating component of the information superhighway [5]. It is also clear that unfettered access to content requires that content providers be able to maintain control over literary or copyrighted assets. Many analysts conclude that this will be one of the key bottlenecks in the implementation and deployment of New Media.

2 Information Commerce and Digital Value Chains

Information commerce is often considered a wholly new concept, made possible only through the use of networks and computers. In fact, a robust information economy has existed for centuries, involving trafficking in physical *representations* of information such as books, newspapers, and so on. Because such commerce involves physical goods, there is a non-negligible floor to the cost of handling information goods. The new aspects of the electronic information economy are that the information itself is the entire product and that the product can be distributed at negligible marginal cost.

The traditional information economy in physical goods is publisher-centric, because creation of information goods—particularly low-cost goods—

requires a substantial manufacturing investment. Figure 1 illustrates a simplified traditional information economy: physical goods flow from a publisher (manufacturer) to a customer, in response to orders and followed by payments. The author's relationship with the publisher may be more lightweight, but the author is nonetheless dependent on the publisher to report sales and make royalty payments in accordance with the author's contract. In addition, a financial institution provides payment processing and clearing services for all parties.

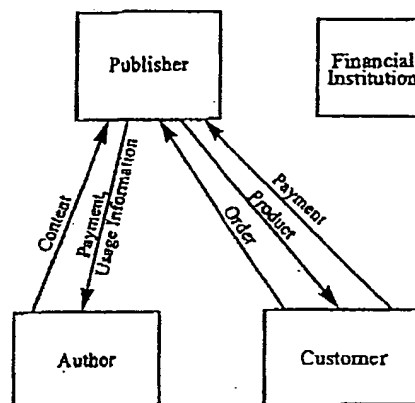


Figure 1. Traditional information economy.

Because of the flexibility afforded by electronic mechanisms, information commerce is evolving from indirect, advertiser-supported, mass-audience media to a new, niche-audience-oriented business model. In this system, members of the electronic community, with or without the economic support of advertising, pay providers directly for what they want to receive. Business-to-business purchasing is steadily evolving into a direct electronic ordering model.

Figure 2 illustrates the flexibility possible in new electronic information commerce models. Although there is still a role for publishers, this role no longer involves physical goods. Rather, the publisher is responsible for packaging and aggregating information goods and control information,

then making them available to customers. Similar to a manufacturing/distribution/retail chain for physical goods, the electronic model permits information retailers, and even end customers, to repackage and redistribute different aggregations of information while ensuring that the appropriate control rules are maintained. A clearinghouse ensures that usage information and payments are provided directly to authors and publishers; the payments themselves are made through traditional financial institutions. Because control rules are associated with information, a variety of payment and other business models can be associated with the same content (e.g., *purchase versus pay-per-use*).

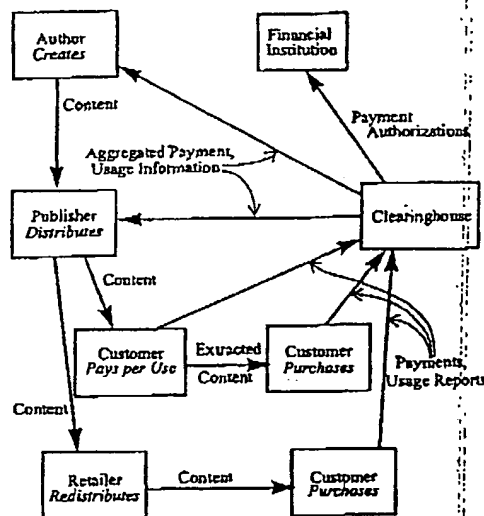


Figure 2. Electronic information economy.

The conversion from traditional commercial distribution channels requires key foundation technologies and results in a fundamental shift in existing infrastructures. This channel transformation will create a new electronic digital distribution industry. Digital distribution employing the DigiBox container architecture and its associated support environment, InterTrust™, can play a critical role in this transformation of the communication, media, and information technology markets.

2.1 Protecting All the Information in Information Commerce

The very properties that make "the net" attractive as a distribution medium—ease of manipulating information in electronic form—also appear to make these protections intractable. Addressing this dichotomy requires a paradigm shift in computer architecture to introduce the concept of a "secure processing" environment in which protected information can be manipulated without being subject to external tampering or disclosure. A prerequisite to such an environment is a cryptographically protected "container" for seamlessly packaging information and controls that enforce information use rights.

The DigiBox described by this paper is such a container.

The need for various information commerce computers and appliances to interoperate requires that this container format and its access methods be standardized. EPR has submitted initial specifications for the DigiBox container to the American National Standards Institute (ANSI) Information Infrastructure Standards Panel (IISP) through the Electronic Publishing Task Force (EPUF) in the User/Content Provider Standards Working Group (WG4).

The primary goal of information protection is to permit proprietors of digital information (i.e., the artists, writers, distributors, packagers, market researchers, etc.) to have the same type and degree of control present in the "paper world." Because digital information is intangible and easily duplicated, those rights are difficult to enforce with conventional information processing technology. Many types of rights (compensation, distribution, modification, etc.) are associated with the various elements of information commerce, and these information property rights take many forms. At a high level, there is the legal definition of "copyright," codified in U.S. law [6–9] and the Berne Convention. This gives copyright holders a legal right to control how copyrighted information is handled. In addition, various high-level rights are conferred by contractual arrangements between primary rightsholders and other parties.

For example, the protections needed for content elements incorporate the licensing provisions for the intellectual property rights of the content rightsholders. In a broader sense, these rights include control over several activities: the right to be compensated for use of the property; the right to control how content is distributed; the right to prevent modification of content by a distributor; "fair use" rights; the rights to the usage data, privacy rights of individuals, and so on.

In the realm of physical goods, these rights are enforced by a combination of legal and technical means. However, the technical means can be (and are) unsophisticated because the technology for violating rights is relatively expensive and time-consuming—in comparison to equivalent activities with respect to digital information. Photocopying a book or copying a video cassette is inherently more labor intensive and costly than copying a file. So, while defeating technical means of enforcement is (relatively) expensive, it can be done—and often the legal means to deter this are inadequate.

2.2 Information Commerce—Not Just Payment

Rights protection is also a fundamental aspect of commerce. Commerce is not just a way for two parties to pay each other for something. Rather, it is an extraordinarily rich web of relationships among parties that concerns payment, negotiation, control, advertising, reporting, auditing, and a variety of other activities. These activities are important aspects of the transaction relationships. Often the information carried in these reports, audits, and the like is highly valuable and highly confidential, perhaps even more valuable than the content that is the subject of the information commerce at hand. These activities too are performed and controlled in the "paper world" by legal and technical means, but there are no widely used models for their electronic equivalents.

Figure 3 shows some of the operations that could occur in true electronic commerce, using the Internet World-Wide Web [10] mechanisms as an example. Creators originate content and apply rules (e.g., "pay author \$1.00/use") for its use. Distributors repackage content, applying additional rules

(e.g., "pay \$5.00 for the collection, then pay the creator," "report use of each item"). Users receive content and operate on it, generating billing reports and usage reports that are delivered to a clearinghouse and paid or summarized back for the originating parties. This structure is very rich and is capable of supporting many business models. There are multiple flows of information in many different directions amongst the parties involved in the transactions.

Another example is that of an advertiser (acting as distributor, or with a distributor). The advertiser might have a rule that offers a discount, or no charge at all, but only if the user views the advertisement and agrees to have that fact reported to the advertiser.

It is relatively simple to devise schemes for parties to pay each other electronically (for example, DigiCash [11], NetBill [12], Open Market [13], SNPP [14], NetCheque [15], First Virtual [16], etc.). Payment, however, constitutes only one—and perhaps the simplest one—of the means in which parties in commerce interact. All the other information commerce components must be accomplished with the same needs for security, privacy, and integrity. In fact, these aspects of electronic commerce, including rights protection, are strongly intertwined in the digital economy, because much digital commerce concerns information and innovative business models for information commerce.

3 Existing Approaches to Information Commerce

Information proprietors employ a variety of technological protection approaches today. These approaches are generally "point solutions," in that they protect a specific type of property in a specific context and enforce only specifically defined rights—typically only the right to compensation for use. Because the technologies are limited, the market is fragmented, and there are no general protection solutions.

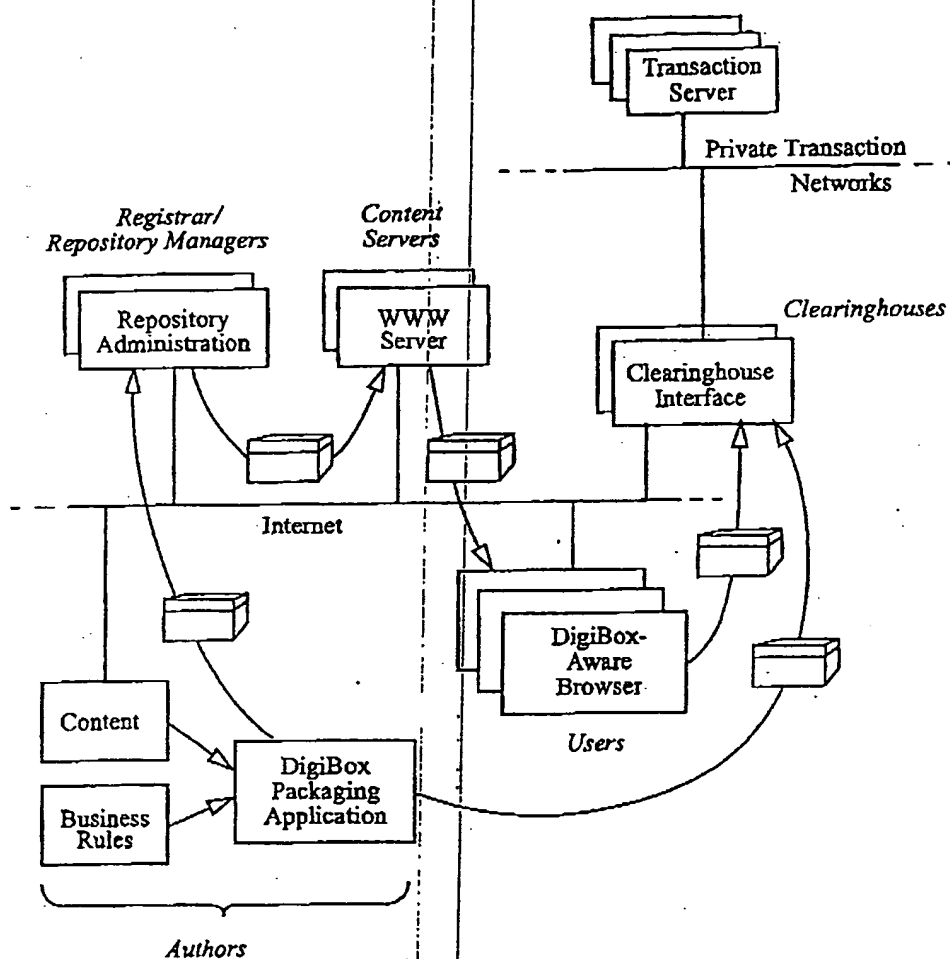


Figure 3. Multi-party Internet information commerce.

3.1 No Protection

Much digital property is distributed without any technological enforcement for property rights, on the assumption that legal means suffice. This approach works well enough for many low-value properties, but it has the disadvantage of raising the price to legitimate users who must pay for both

their own and illegitimate use. In many cases, however, this cost is negligible, and no protection is an economically sound choice. Even for content that is free, however, a creator may wish to impose some rules for reporting or some access control. Of course, privacy rights of users will be a concern to many.

3.2 License Managers

For some valuable software properties, license managers are used. Because a software property is dynamic (executable), it is feasible to restrict it so that it functions properly only through interaction with a license manager process. In general, there is no protection of usage data in these schemes. In some cases this technique has been applied to content protection, but only with limited success [17, 18].

3.3 Cryptographic Unlock

Some static properties (fonts, for example; also some installable software) are protected by a simple "unlock" scheme: a purchaser makes a purchase, for example by telephone with a credit card, and receives a cryptographic key in return. This key can then be used to "unlock" one property from some widely distributed medium (e.g., CD-ROM or network download). This mechanism is relatively inflexible, and its inherently manual nature makes it expensive.

3.4 Billing Schemes

Various billing schemes (as mentioned above) permit purchase of information following what is essentially an electronic check or electronic credit draft model. These methods are suitable for conventional transactions, but not for the enormous volumes of (individually) very low-value transactions that would be generated using a complex digital property.

3.5 Secured Delivery

Various secured delivery systems (e.g., SSL [19], SHHTTP [20]) share the same problems as cryptographic unlock, but in a network context. They are only point-to-point solutions, with the information (content, usage data, etc.) at each site being left unprotected once the delivery has occurred. Furthermore, they are inherently online systems: it is not practical to decouple the delivery of information from payment for its use.

4 Information Protection Architecture: InterTrust and DigiBox

EPR has produced the InterTrust Virtual Distribution Architecture to solve unmet, critical needs of electronic commerce. Almost any imaginable information transaction can be supported by InterTrust. A few examples include distribution of content (e.g., text, video, audio) over networks, selective release of data from a database, controlled release of sensitive information, and so on. InterTrust can also support the secure communication of private information such as EDI and electronic financial transactions, as well as delivery of the "back channel" marketing and usage data resulting from transactions.

DigiBox is a foundation technology within InterTrust. It provides a secure container to package information so that the information cannot be used except as provided by the rules and controls associated with the content. InterTrust rules and controls specify what types of content usage are permitted, as well as the consequences of usage such as reporting and payment.

Within InterTrust, DigiBox containers can enforce a "distributed electronic contract" for value-chain activities functioning within an electronic distribution environment. This unique approach underlies EPR's information metering and digital rights protection technology. Electronic commerce infrastructure participants can use InterTrust to substantially enhance their network, security, or payment method solutions.

The DigiBox is a container for both digital property (content) and controls. It is used in conjunction with a locally secured rights protection application (discussed further below) to make content available as governed by arbitrarily flexible controls.

The DigiBox container mechanism is implemented in a set of platform-independent class libraries that provide access to objects in the container and extensions to OpenDoc and OLE object technologies. DigiBox allows rights management components to be integrated with content in highly flexible and configurable control structures. Digi-

Box rights management components can be integrated with content in a single deliverable, or some or all of the components can be delivered independently. DigiBox rights management components enable true superdistribution [21] and can support virtually any network topology and any number of participants, including distributors, redistributors, information retailers, corporate content users, and consumers.

4.1 Content

The digital information in a DigiBox (one or more "properties") is information in any form. It may be mapped to a specific compound object format (e.g., OpenDoc, OLE, PDF), or may be application specific.

Further, it may be delivered in stream or other communication-oriented forms, not just in a file-like container.

4.2 Controls

Controls specify rules and consequences for operations on content. Controls are also delivered in a DigiBox, and the controls for a property may be delivered either with the property or independently. Controls are tied to properties by cryptographic means.

Because controls can be delivered with properties in a container, the DigiBox supports superdistribution.

4.3 Commerce

Commerce takes place governed by controls. This may involve metering, billing for use, reporting of usage, and so on. These operations take place locally in a secure environment, and they generate audit trails and reports that must be reported periodically to clearinghouses.

5 DigiBox Implementation

The DigiBox is a structure that can hold, in a protected manner, information commerce elements of all kinds: content, usage information, representa-

tion of financial transactions (e.g., electronic cash), and other digital elements of information commerce.

5.1 Container Logical Structure

Figure 4 shows the logical structure of properties and control sets in two containers. Container C_1 holds two properties, P_1 and P_2 , and one control set, CS_1 , that applies to property P_1 ; container C_2 contains two control sets and no properties. As shown in the example, each of these elements has a title attribute to provide a human-readable description of the element and, for control sets, an attribute indicating to what other elements the control set applies.

A control set specifies rules and consequences, such as pricing, reporting, and so on, for the properties to which it applies. A user holding just this container could use (e.g., view, print) content from P_1 though only as specified by CS_1 . Because there is no control set applying to P_2 in that container, P_2 would not be usable in any way.

A user holding both containers could use property P_2 as specified by CS_2 , and in addition has the choice of whether to designate CS_1 or CS_3 when using P_1 . CS_3 , which describes itself as "discount," is likely to be the user's preferred choice.

The DigiBox includes several elements: organizational structures, properties, controls, and supporting data items. Almost all the information in a DigiBox is encrypted, as described below, and access to the encrypted form is provided through a storage manager as appropriate, depending on how the DigiBox is delivered (e.g., as a file or as a data stream).

5.2 Container Physical Structure

Figure 5 is a schematic picture illustrating the physical structure of a DigiBox container. (Some elements have been omitted for clarity.) It begins with a container header structure containing descriptive and organizational information about the container. Part of the container header is encrypted (both for secrecy and for integrity protection); the rest is public organizational informa-

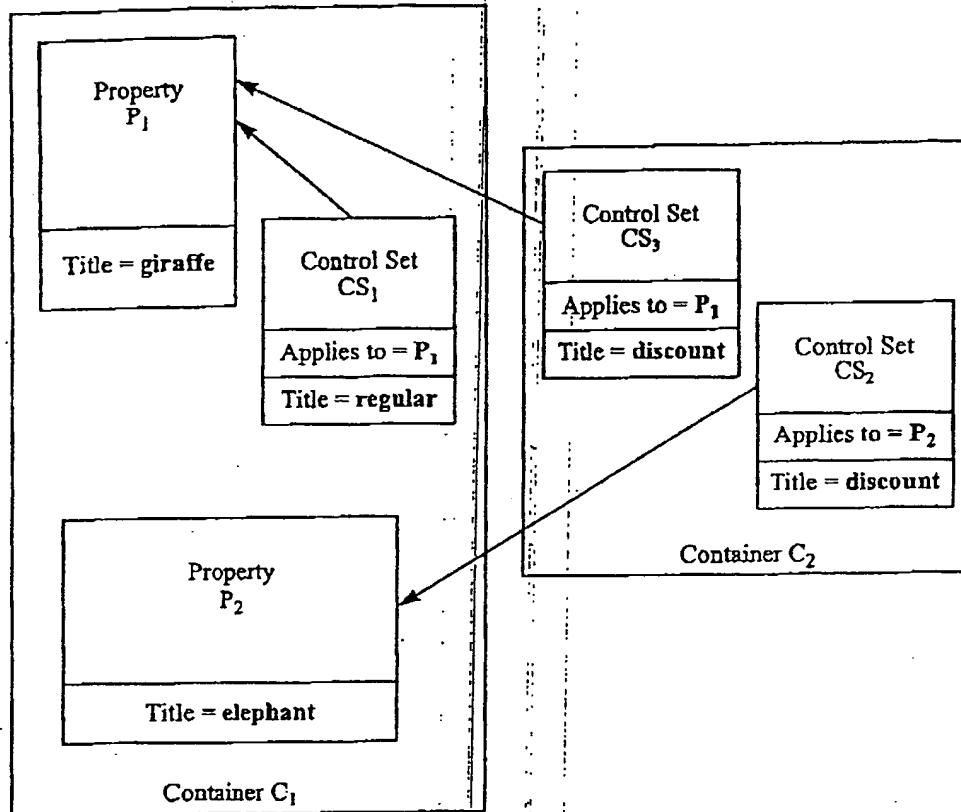


Figure 4. Container logical structure.

tion. The header is followed by additional container-wide structures such as the *transport key block (TKB)* and the *container table of contents (TOC)*, some of which are encrypted and others not.

These organizational elements are followed by the structures defining the container's content (e.g., *properties* and *control sets*). As shown in the figure, a property is represented by a *property header*, *property attributes*, and data blocks composing the property. As shown, the header is encrypted and

the attributes are not; the data blocks may be wholly or partly encrypted, or not at all, depending on security requirements.

The figure shows an example property consisting of a multimedia property formed from a pair of synchronized data streams for audio and video. In this example, each video block is mostly unencrypted so that access can be rapid while still maintaining reasonable security—encrypting even 10 percent of an MPEG stream renders it effectively useless for illicit copying. On the other hand, the audio is entirely encrypted, and each audio block

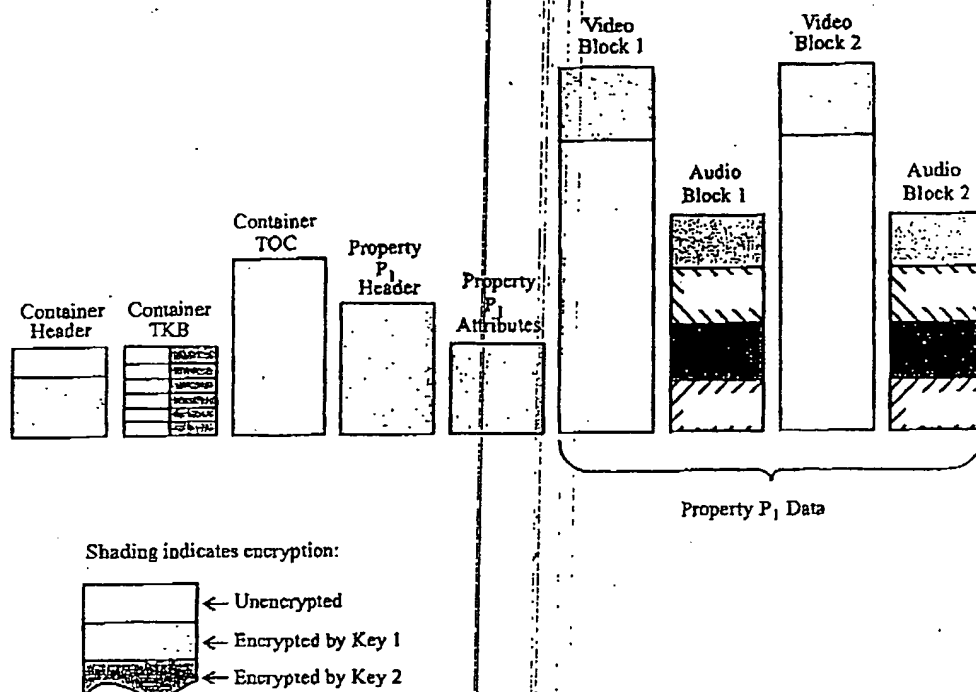


Figure 5. Container physical format.

uses four distinct keys, because the content proprietor requires much stronger security for audio than for video.

A property is represented as one or more property sections, each of which is independently associated with control information, and which may also be stored and accessed independently. A property, for example, might be a collection of clip-art images, and each image might be a property "chunk," with its own control specifying how that image's creator is compensated.

Controls can map to property chunks at arbitrary granularity and can enforce arbitrary organizational structures within the property (such as a file hierarchy). Controls can apply to individual bytes,

frames of a movie, segments of a musical piece, and so on, because the mapping is performed by a control process specified by the control structure, not simply via a table-driven data structure.

5.3 Cryptographic Techniques

The high-level elements in a DigiBox are encrypted with a *transport key* that is normally derived (by exclusive OR) from two parts: one that is delivered in the DigiBox itself, encrypted with a public key algorithm, and the other that is stored in protected storage locally. The locally stored part is shared among all the local nodes capable of processing that DigiBox, but the part in the DigiBox is unique. This separation provides protection against accidental or malicious disclosure of either part.

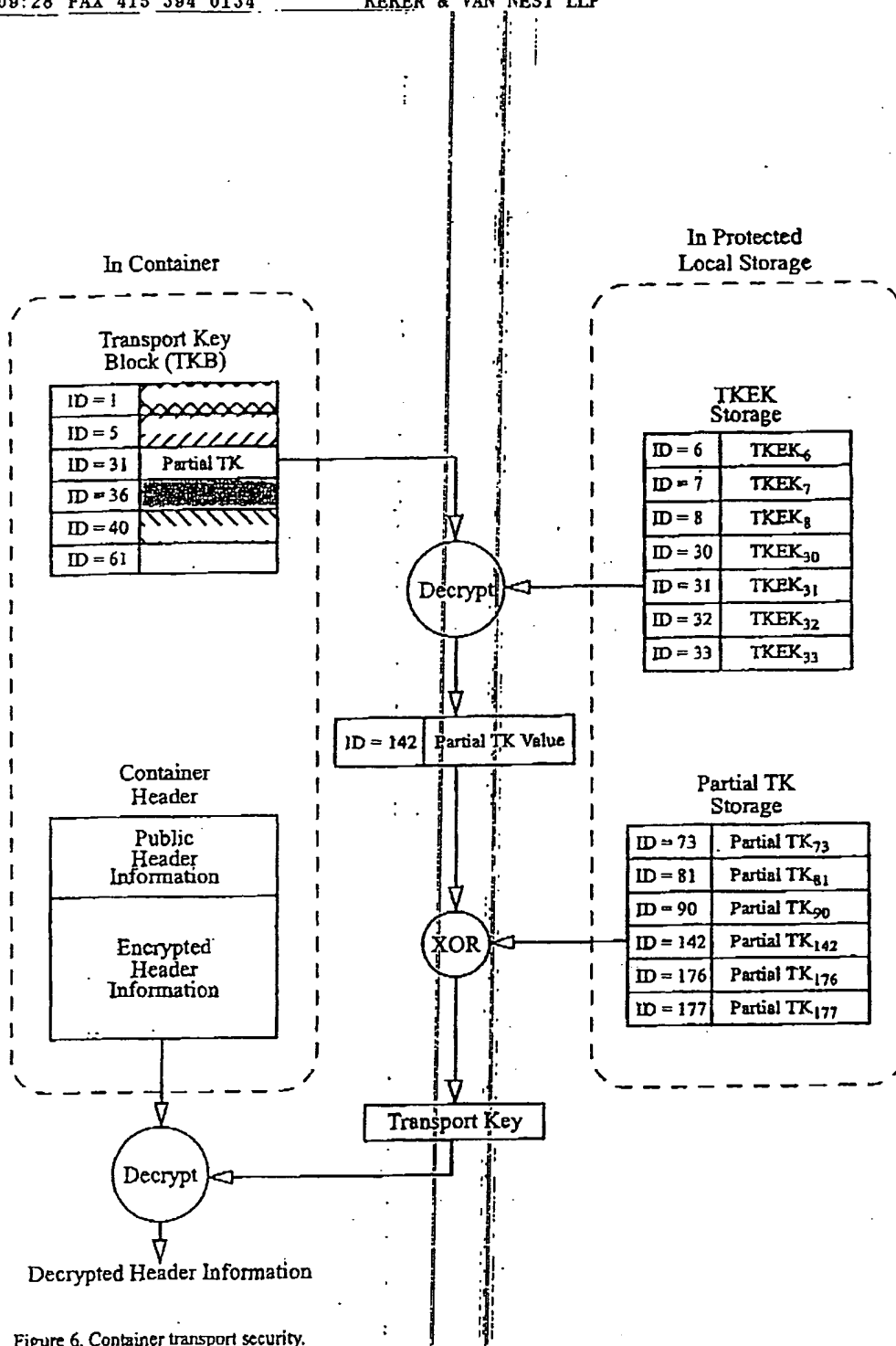


Figure 6. Container transport security.

Figure 6 illustrates how the transport key (TK) is derived. The transport key block (TKB) contains one or more slots, each of which contains a partial

transport key encrypted under a different transport key encrypting key (TKEK). Each TKB slot identifies the TKEK used, and a matching TKEK is

selected from local protected storage. Decrypting the slot yields a partial TK, which is combined with its corresponding partial TK again from protected local storage to yield the actual TK for decrypting the container header.

The data for the property itself is encrypted with other keys ("content keys") that are themselves delivered in encrypted high-level structures; this approach permits the keys for a property to be delivered entirely separately from the property or its controls. Multiple keys, in a wide variety of key-mapping schemes, are used to encrypt the data, limiting the loss that would occur from disclosure of any one key.

All DigiBox control structures are both encrypted and verified for integrity with a cryptographic hash function. Several cryptographic algorithms are supported for these control structures (principally for export control reasons), and arbitrary algorithms are supported for encryption of the data.

5.4 Security Characteristics

The DigiBox cryptographic structures are designed to be secure even in the face of loss of individual key components, and to minimize the damage in case a key or processing environment is compromised. The system is designed to provide commercially acceptable risks and losses for a variety of business models.

The basic algorithms are strong: Triple DES [22] and RSA [23] are preferred. This security, is, of course, only as strong as the tamper-resistance of the local processing environment. The preferred implementation of DigiBox processing relies on a "secure processing unit" (SPU) that contains a CPU, memory, program storage, and key storage in a single tamper-resistant hardware package. Although these are not widely available today, the variety of applications they might support makes it likely that such SPUs will become widely integrated into common computing platforms. When running in an SPU, the DigiBox processing and control mechanisms are sufficiently well protected to support most commerce applications.

In the absence of an SPU, other approaches are useful for many business models. In fact, a software-only implementation is sufficient for many applications, because much content is of relatively low value and is used in a context (business to business) where a modest level of fraud is both less likely and more tolerable. As long as the software is moderately difficult to defeat and tools to defeat it have no legitimate purpose, business models can be supported where some risk of loss is acceptable. In the world of electronic commerce, just as for traditional commerce, security is not absolute: it is just a factor to balance against the cost of loss and fraud.

6 Conclusions

The DigiBox is one component of a general-purpose electronic commerce solution that rests on three basic principles: rights protection, interoperability, and strong security.

Electronic commerce, and information commerce in particular, needs a robust information protection mechanism, including rights protection and controls, not just payment systems. As the electronic world evolves, however, and moves forward from simply emulating traditional transactions into entirely new business models, rights protection and control will become the predominant issues.

Protection of intellectual property rights in information requires strong cryptography as well as a flexible infrastructure for controlling use of the information. A standard protected container for information is necessary to support interoperability—most existing schemes tightly bind the creator of protected information and the software that processes it. A standard container can rationalize information commerce and reduce costs for all participants.

In the long term, general-purpose secure electronic commerce will need pervasive deployment of tamper-resistant hardware devices to perform secure processing of protected content. However, as these solutions are developed, many business models can be accommodated with weaker or less complete solutions because the risk and expected losses are commercially acceptable.

Business-to-business purchasing is steadily evolving into a direct electronic ordering model. Future communications and media markets will become increasingly segmented and specialized in response to customer preferences and needs and involve increasing, and more sophisticated, direct interaction between consumers and providers. These markets and their value chains (with or without intermediary distributors) will require secure metering and control tools that enable a user to efficiently and economically tailor resources to his or her own desires.

During the next decade, digital delivery of traditional electronic products, such as information databases and software, will be joined by a rapidly growing array of both New Media and electronically distributed traditional content. The conversion from traditional models requires key foundation technologies and will result in a fundamental shift in current infrastructure. This transformation will create a new distribution industry. Digital distribution employing a universal content and commerce container can play a critical role in this broad economic transformation.

7 References

- [1] A. Chandler and H. Daems, "Administrative Coordination, Allocation, and Monitoring: A Comparative Analysis of Accounting and Organization in the U.S.A. and Europe," *Accounting, Organizations and Society*, 1979: 3-20.
- [2] O. Williamson, "The Modern Corporation: Origin, Evolution, Attributes," *Journal of Economic Literature* XIX (1981): 1537-1568.
- [3] Office of Technology Assessment, *Accessibility and Integrity of Networked Information Collections*. Washington, D.C.: U.S. Government Printing Office, July, 1993.
- [4] E. Hollings, *Communications Competitiveness and Infrastructure Modernization Act of 1990*. Washington, D.C.: U.S. Government Printing Office, report of the Senate Committee on Commerce, Science, and Transportation, 12 September 1990.
- [5] R. Benjamin and R. Wigand, "Electronic Markets and Virtual Value Chains on the Information Superhighway," *Sloan Management Review*, Vol. 36 No. 2 (1995).
- [6] U.S. Constitution, Article 1, Section 8, Clause 8 (1787).
- [7] U.S. Copyright Act of 1978
- [8] 17 U.S.C. §107
- [9] 17 U.S.C. §102(a)
- [10] T. Berners-Lee, R. Cailliau, and J.-F. Groff, "The World Wide Web," *Computer Networks and ISDN Systems*, Vol. 25 (Dec. 1992), pp 454-459.
- [11] D. Chaum, "Achieving Electronic Privacy," *Scientific American*, August 1992, pp 96-101.
- [12] M. Sirbu and J. D. Tygar, "NetBill: An Internet Commerce System," *IEEE CompCon Proceedings*, March, 1995, pp 20-25.
- [13] D. Gifford et al., "Payment Switches for Open Networks," *IEEE CompCon Proceedings*, March, 1995, pp 26-31.
- [14] S. Dukach, "SNPP: A Simple Network Payment Protocol," MIT Laboratory for Computer Science, Cambridge, MA, 1993.
- [15] B. C. Neuman and G. Medvinsky, "Requirements for Network Payment," *IEEE CompCon Proceedings*, March, 1995, pp 32-36.
- [16] First Virtual, Inc. "Introducing the First Virtual Internet Payment System," 1994.
- [17] A. K. Choudhury, et al., "Copyright Protection for Electronic Publishing over Computer Networks," June 1994, *IEEE Network Magazine*.
- [18] J. Erickson, "A Copyright Management System for Networked Interactive Multimedia," *Proceedings of the 1995 Dartmouth Institute for Advanced Graduate Studies*, 1995.

BEST AVAILABLE COPY

09/28/2001 09:29 FAX 415 394 0134

KEKER & VAN NEST LLP

032

- [19] K. Hickman, "SSL Reference Manual," Netscape Corporation World Wide Web Site, <http://www.netscape.com/newsref/std/sslref.html>, 1994.
- [20] E. Rescorla and A. Schiffman, "The Secure HyperText Transfer Protocol," Internet Draft draft-rescorla-shhttp-0.txt, 1994.
- [21] B. Cox, "Superdistribution," *Wired*, Sept. 1994, pp 89-92.
- [22] U.S. National Bureau of Standards, "Data Encryption Standard," *Federal Information Processing Standards Publication*, FIPS PUB 46-1, Jan. 1988.
- [23] R. Rivest, A. Shamir, and L. Adleman, "On Digital Signatures and Public-key Cryptosystems," *Communications of the ACM*, Vol. 21 (Feb. 1978), pp 120-126.

BEST AVAILABLE COPY

09/28/2001 09:29 FAX 415 394 0134

KEKER & VAN NEST LLP

0033

EXHIBIT B

BEST AVAILABLE COPY

09/28/2001 09:30 FAX 415 394 0134

KEKER & VAN NEST LLP

034

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6: G06F		(11) International Publication Number: WO 96/27155
A2		(43) International Publication Date: 6 September 1996 (06.09.96)
(21) International Application Number: PCT/US96/02303		(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MC, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG). Eurasian patent (AZ, BY, KG, KZ, RU, TJ, TM). European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).
(22) International Filing Date: 13 February 1996 (13.02.96)		
(30) Priority Date: 08/388,107 13 February 1995 (13.02.95) US		
(71) Applicant: ELECTRONIC PUBLISHING RESOURCES, INC. [US/US]: 5203 Battery Lane, Bethesda, MD 20814 (US).		
(72) Inventors: GINTER, Karl, L.: 10404 43rd Avenue, Beltsville, MD 20705 (US). SHEAR, Victor, H.: 5203 Battery Lane, Bethesda, MD 20814 (US). SPAIN, Francis, J.: 2410 Edwards Avenue, El Cerrito, CA 94530 (US). VAN WIE, David, M.: 1250 Lakeside Drive, Sunnyvale, CA 94086 (US).		
(74) Agent: FARIS, Robert, W.: Nuzco & Vandehy P.C., 1100 North Glebe Road, Arlington, VA 22201-4714 (US).		Published Without international search report and to be republished upon receipt of that report.

(54) Title: SYSTEMS AND METHODS FOR SECURE TRANSACTION MANAGEMENT AND ELECTRONIC RIGHTS PROTECTION

(57) Abstract

The present invention provides systems and methods for electronic commerce including secure transaction management and electronic rights protection. Electronic appliances such as computers employed in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Secure subsystems used with such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Secure distributed and other operating system environments and architectures, employing, for example, secure semiconductor processing arrangements that may establish secure, protected environments at each node. These techniques may be used to support an end-to-end electronic information distribution capability that may be used, for example, utilizing the "electronic highway".